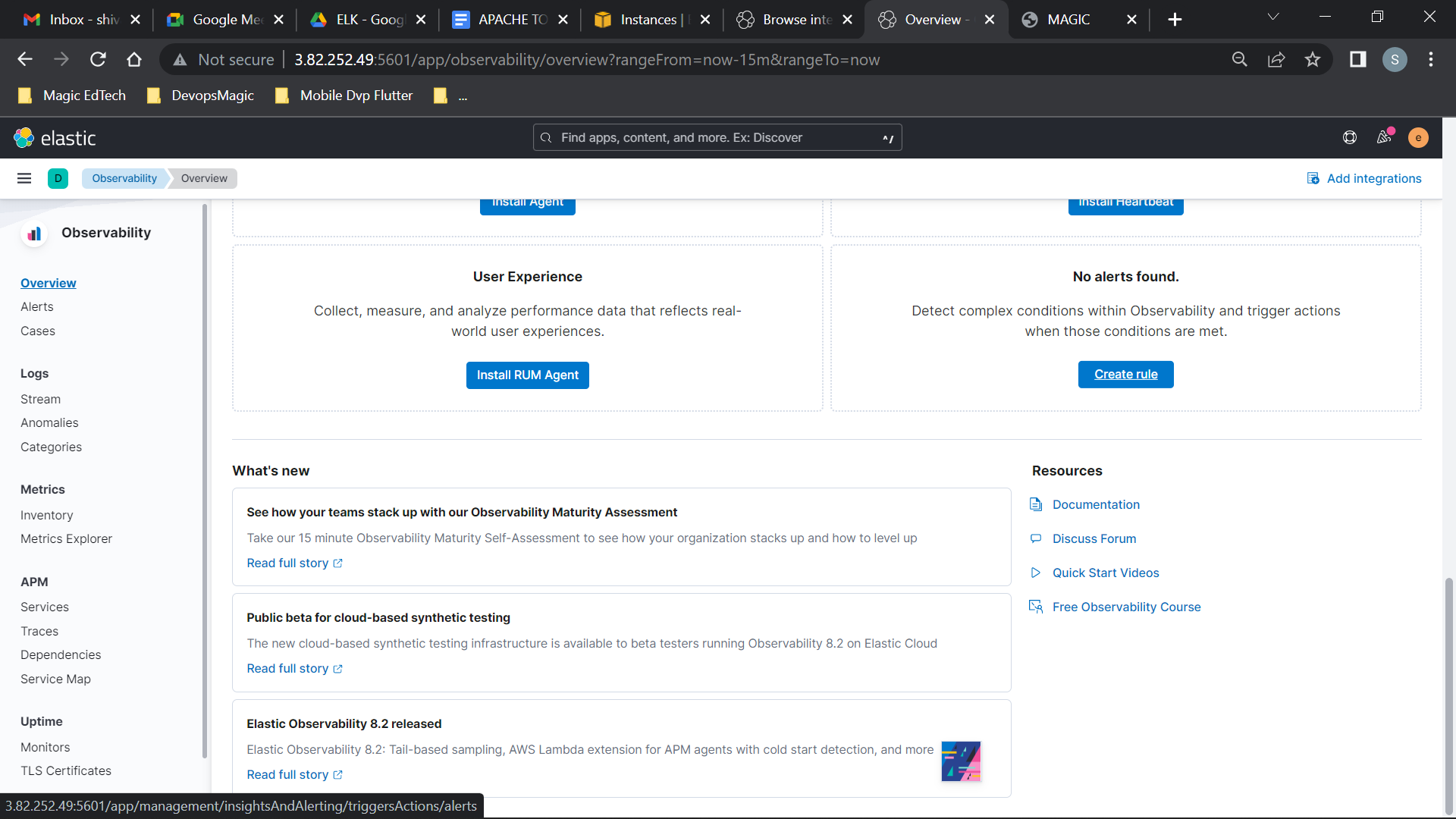
**ALERTS AND RULES**



* + **Create encryption keys:**

cd /usr/share/kibana

sudo bin/kibana-encryption-keys generate

* + **Such type of key value will be generated:**

xpack.encryptedSavedObjects.encryptionKey: xx…………xx

* + **Paste into KIBANA.yml**

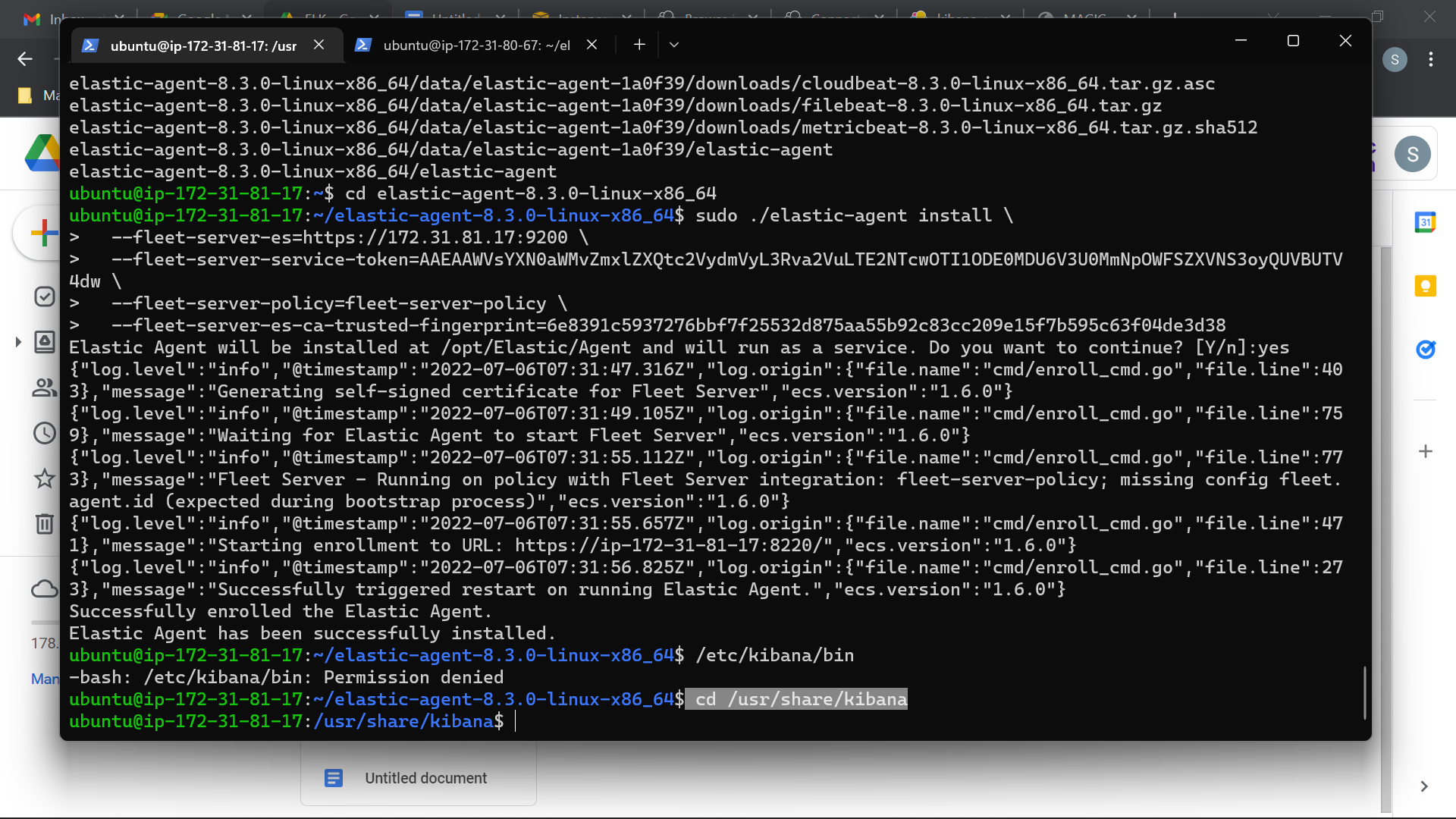
sudo nano /etc/kibana/kibana.yml

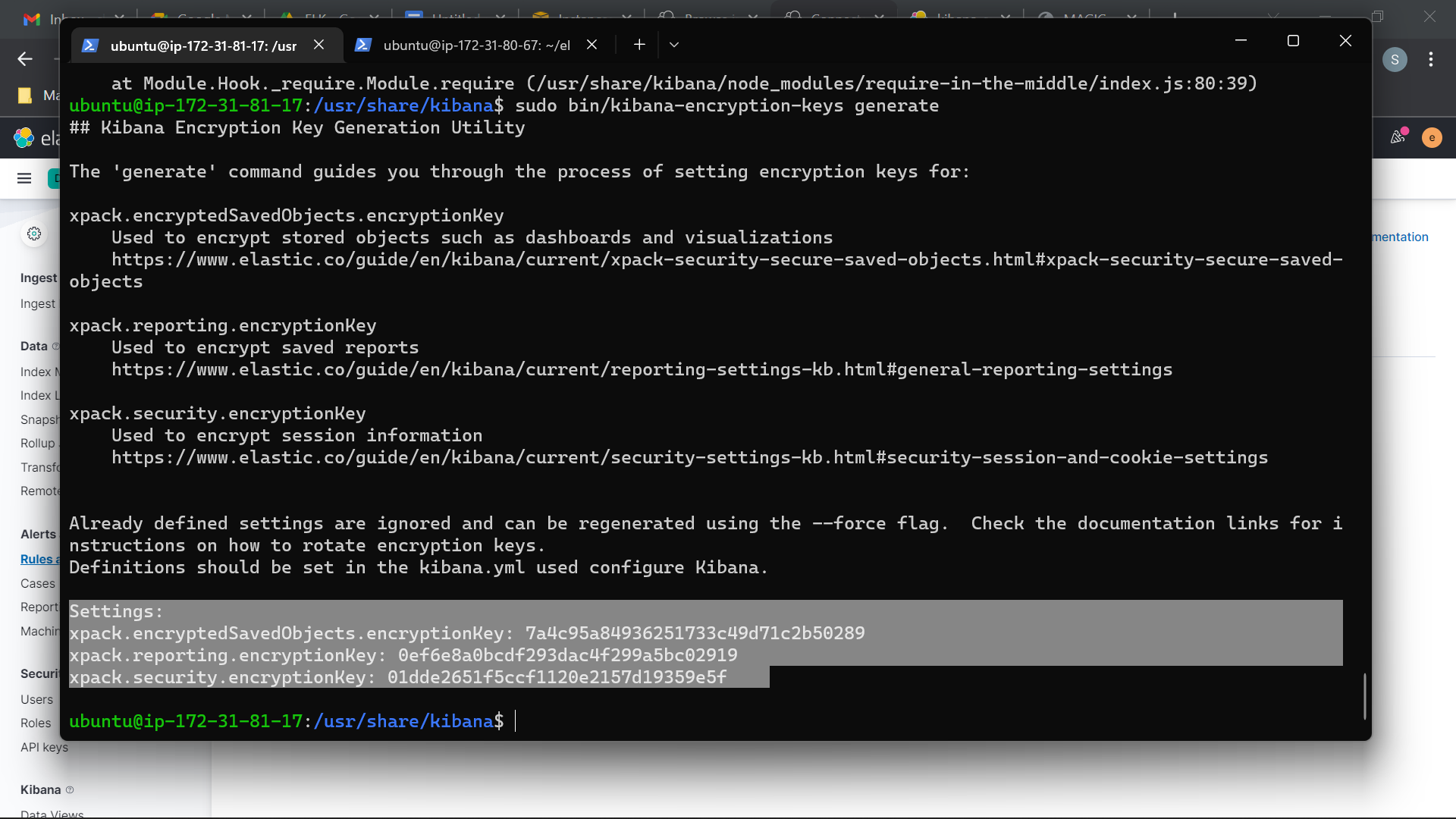
* + **Restart kibana**

sudo systemctl restart kibana.service

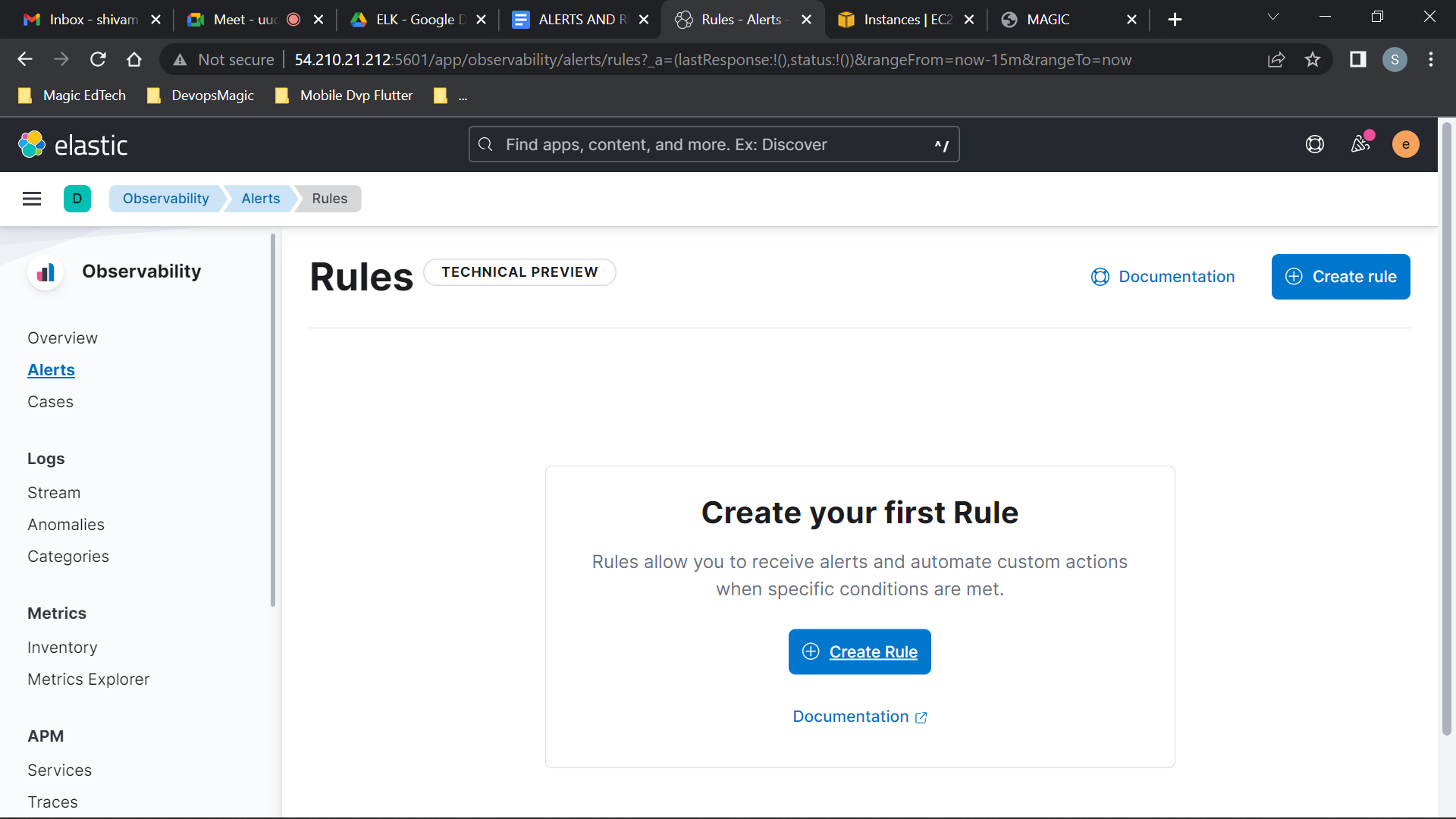
[*https://www.elastic.co/guide/en/kibana/8.3/alert-action-settings-kb.html#general-alert-action-settings*](https://www.elastic.co/guide/en/kibana/8.3/alert-action-settings-kb.html#general-alert-action-settings)

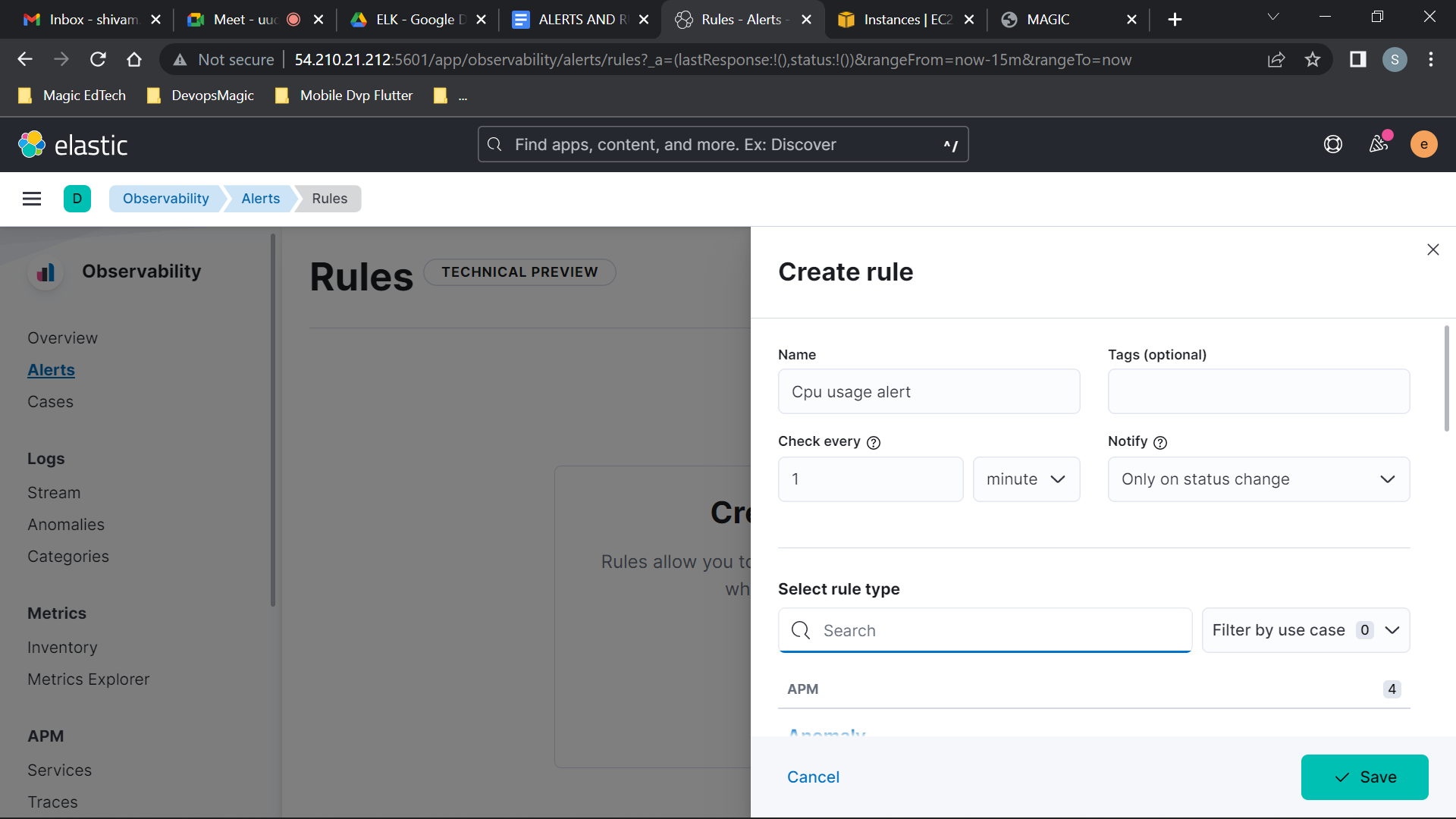
**Reference Images:**



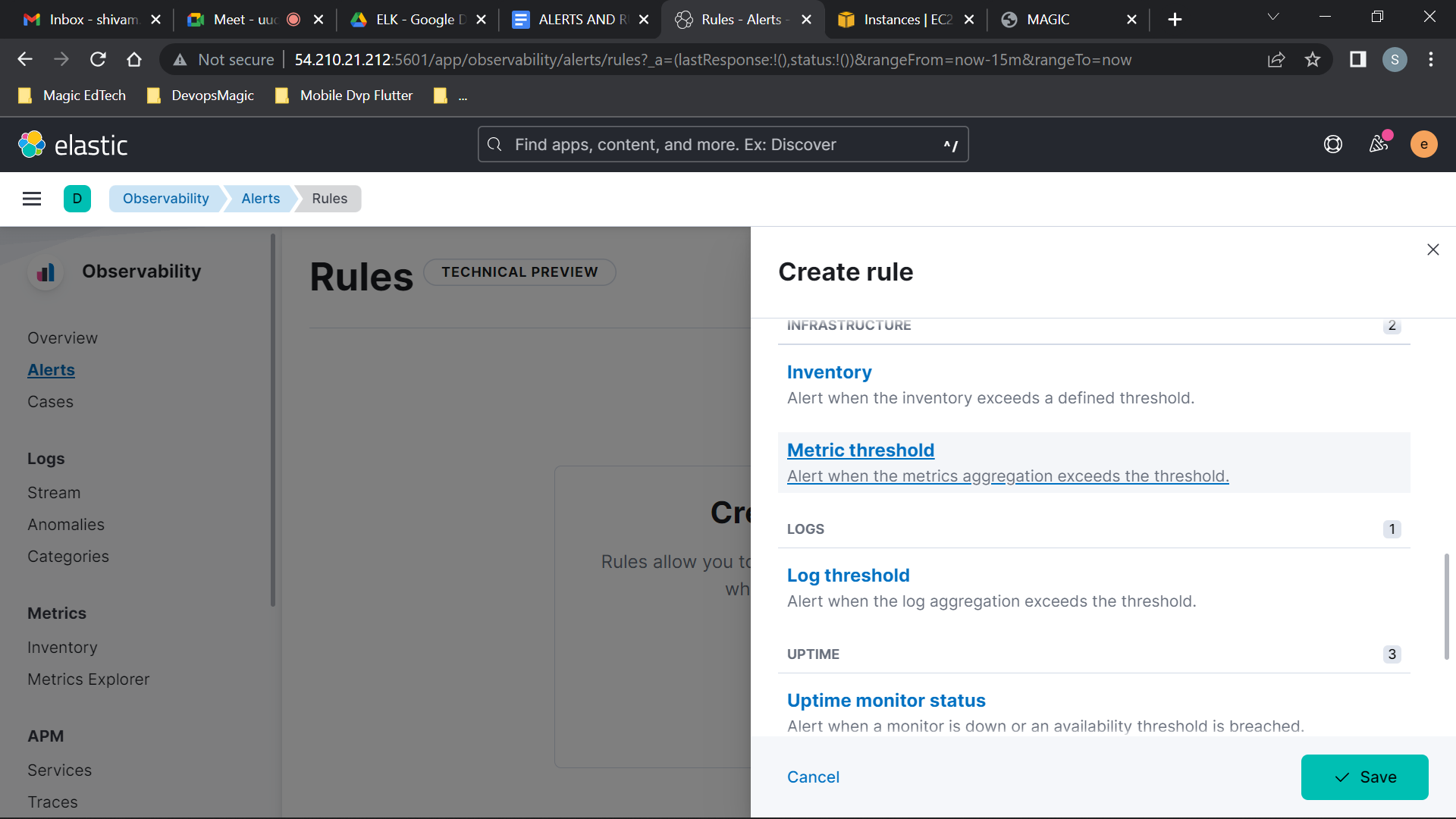


**CREATE RULE FOR ALERTS**

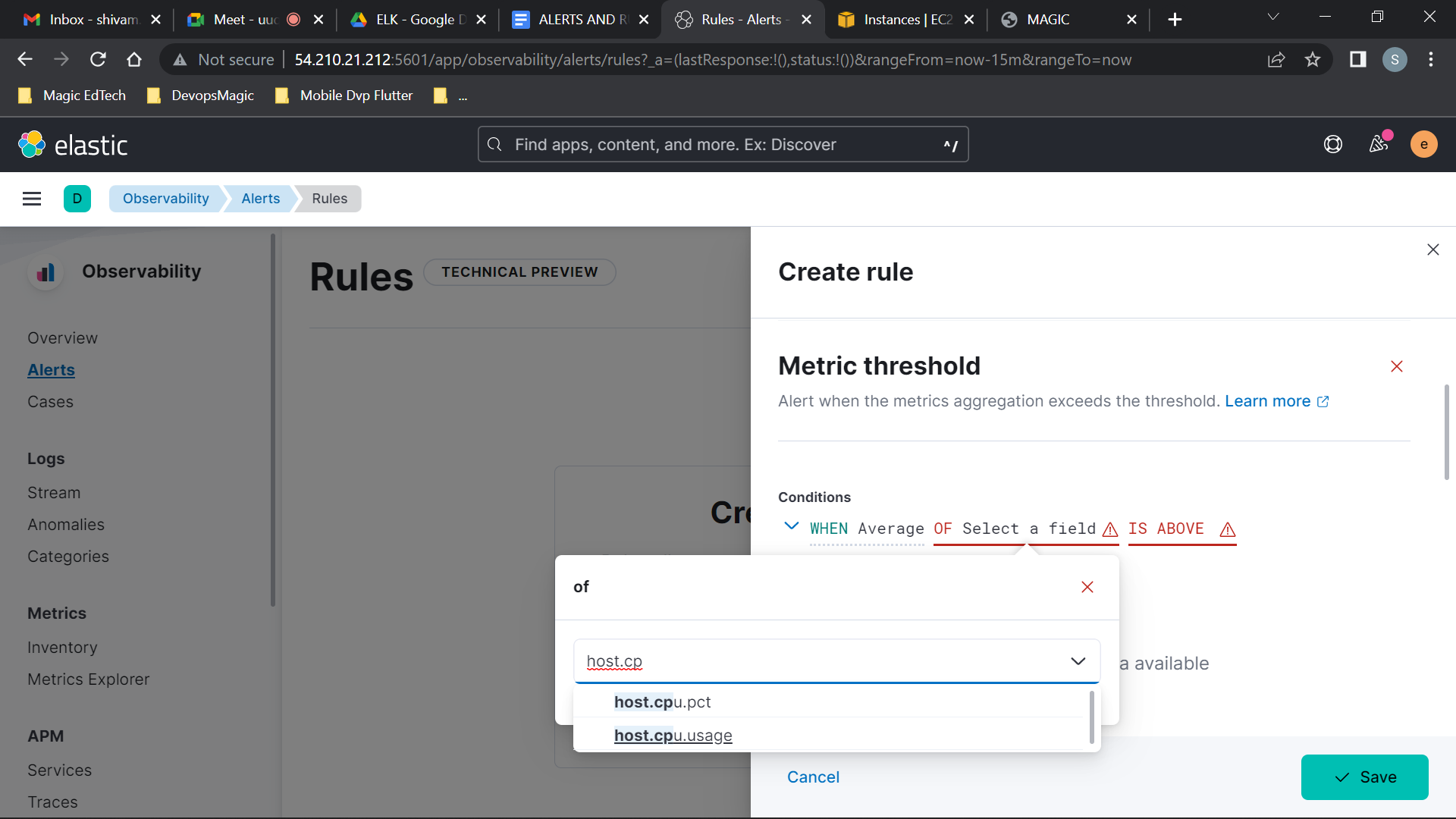
****

****

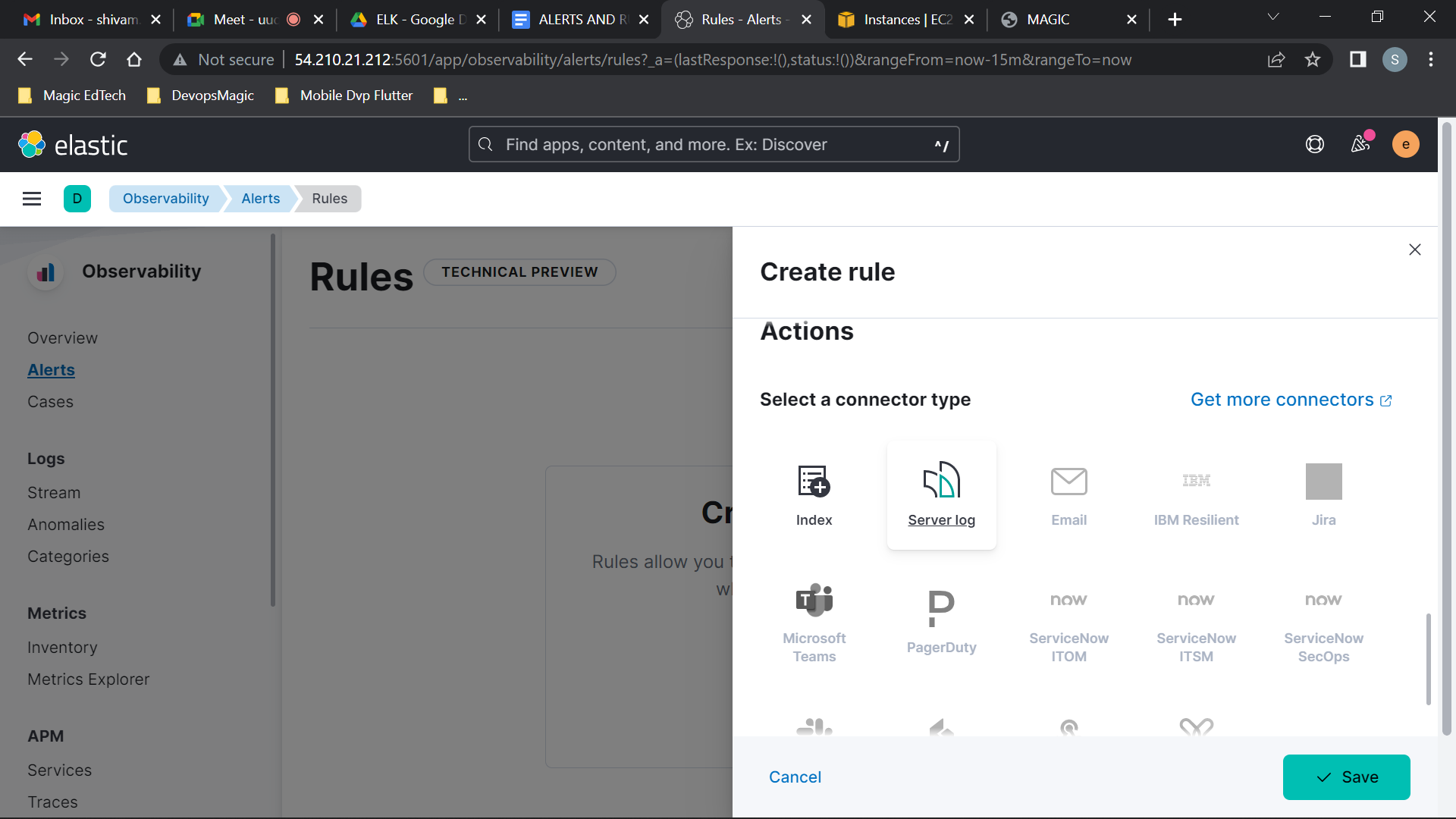
Enter Rule Name and select rule type, in this doc we have used Metric threshold.

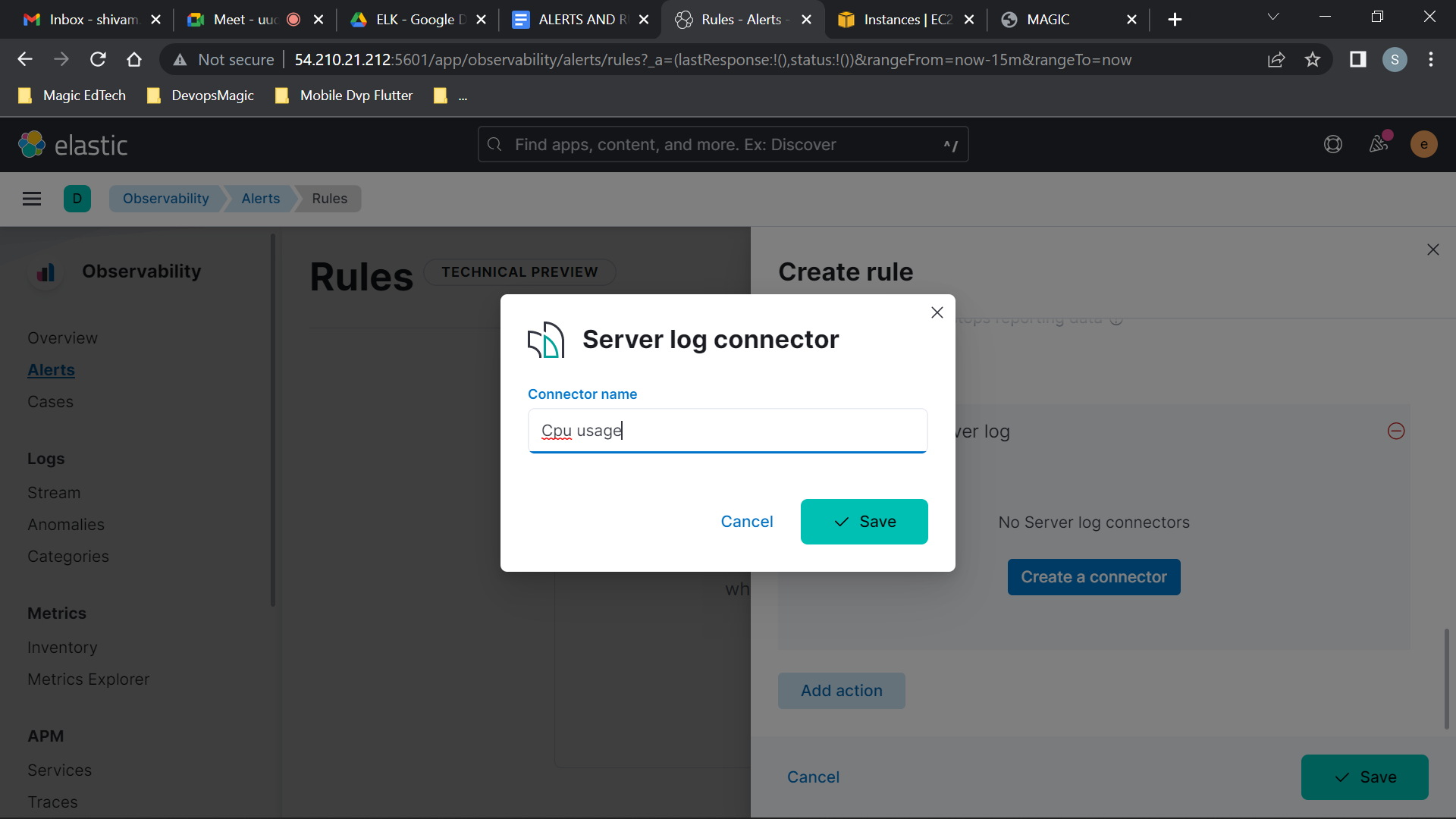
****

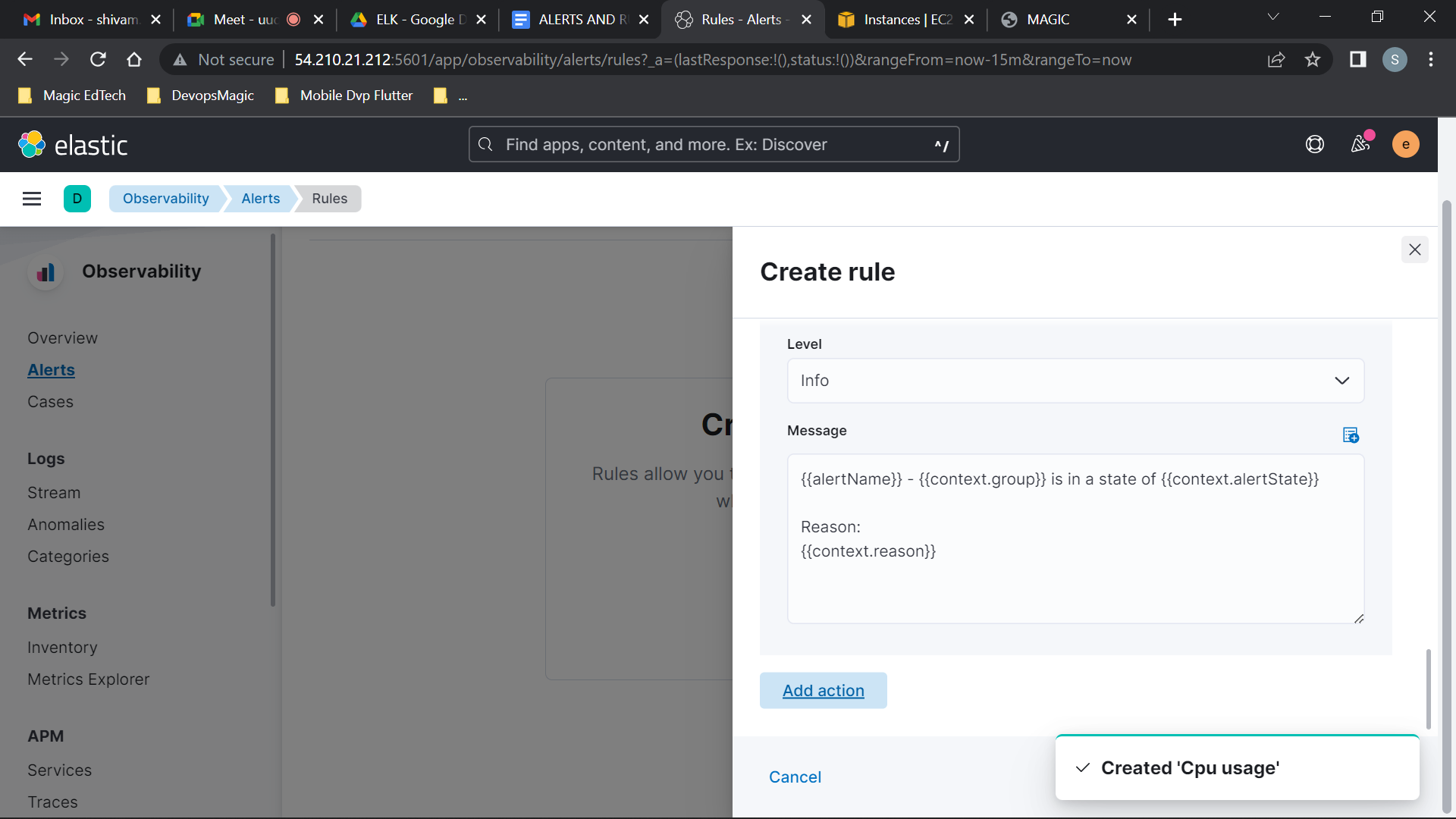
Select a field whose value is crosses the threshold will trigger the alert.

****

Select a Connector

****

****

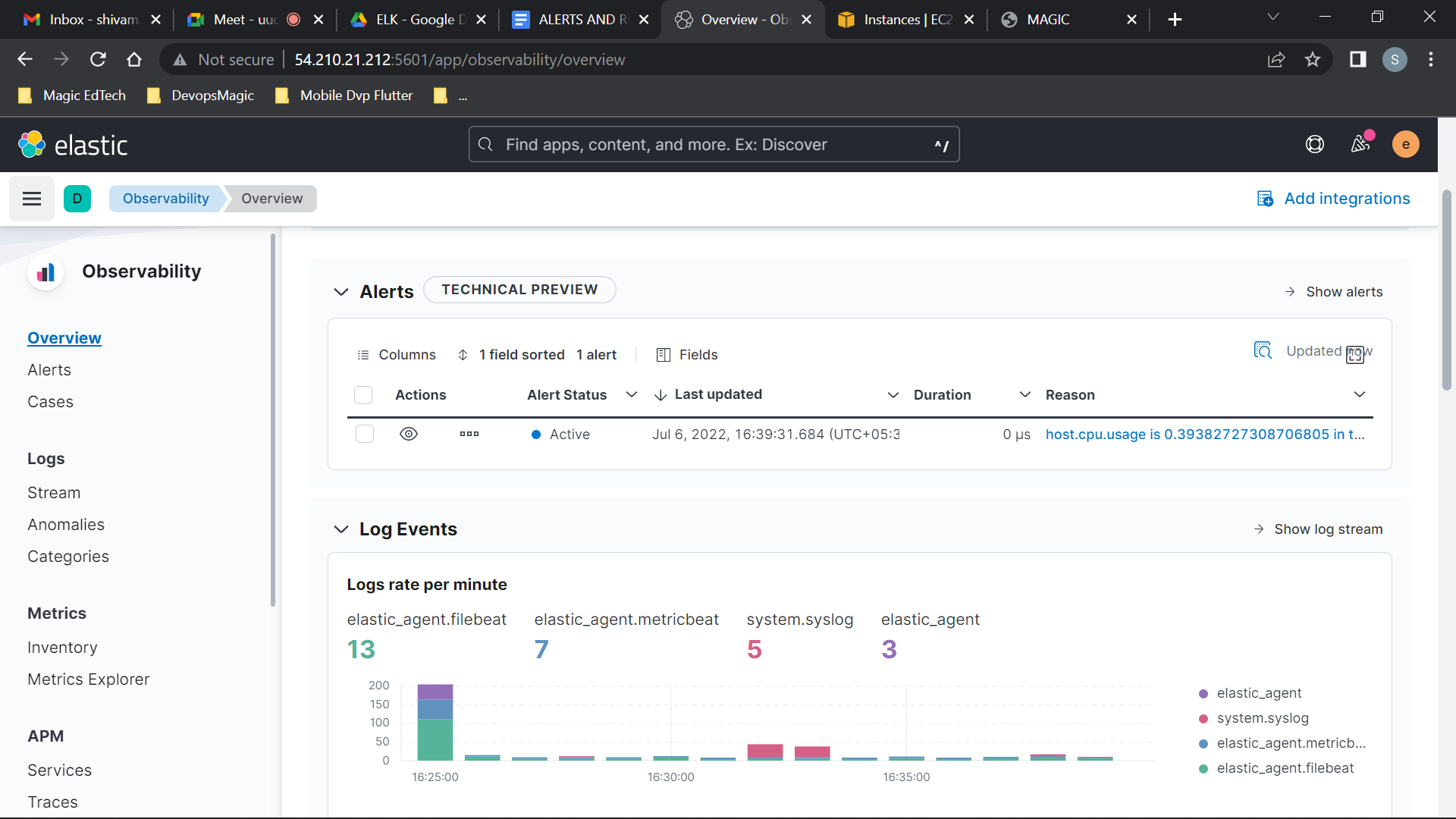
****

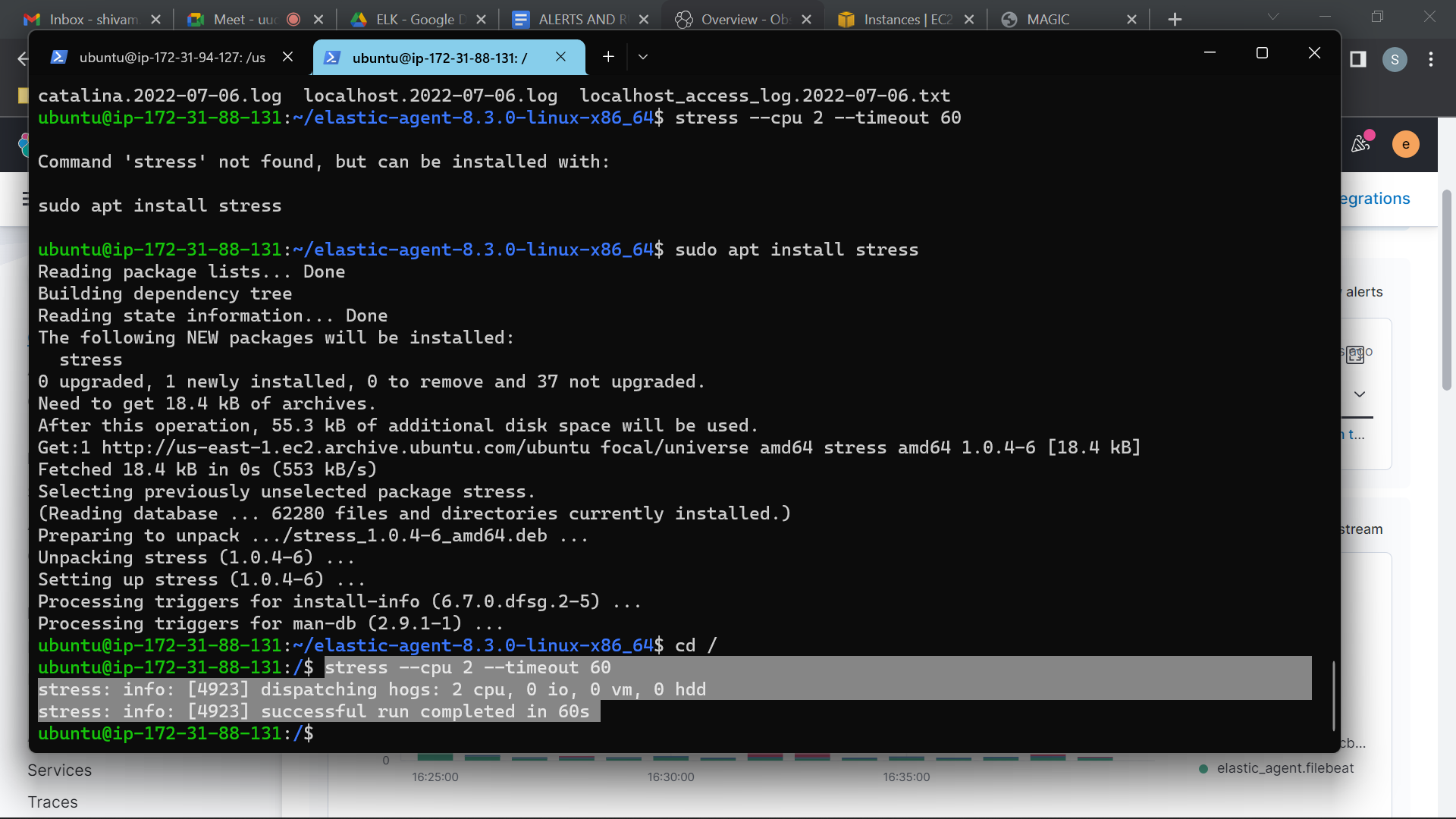
Test the rule by spiking the Cpu usage

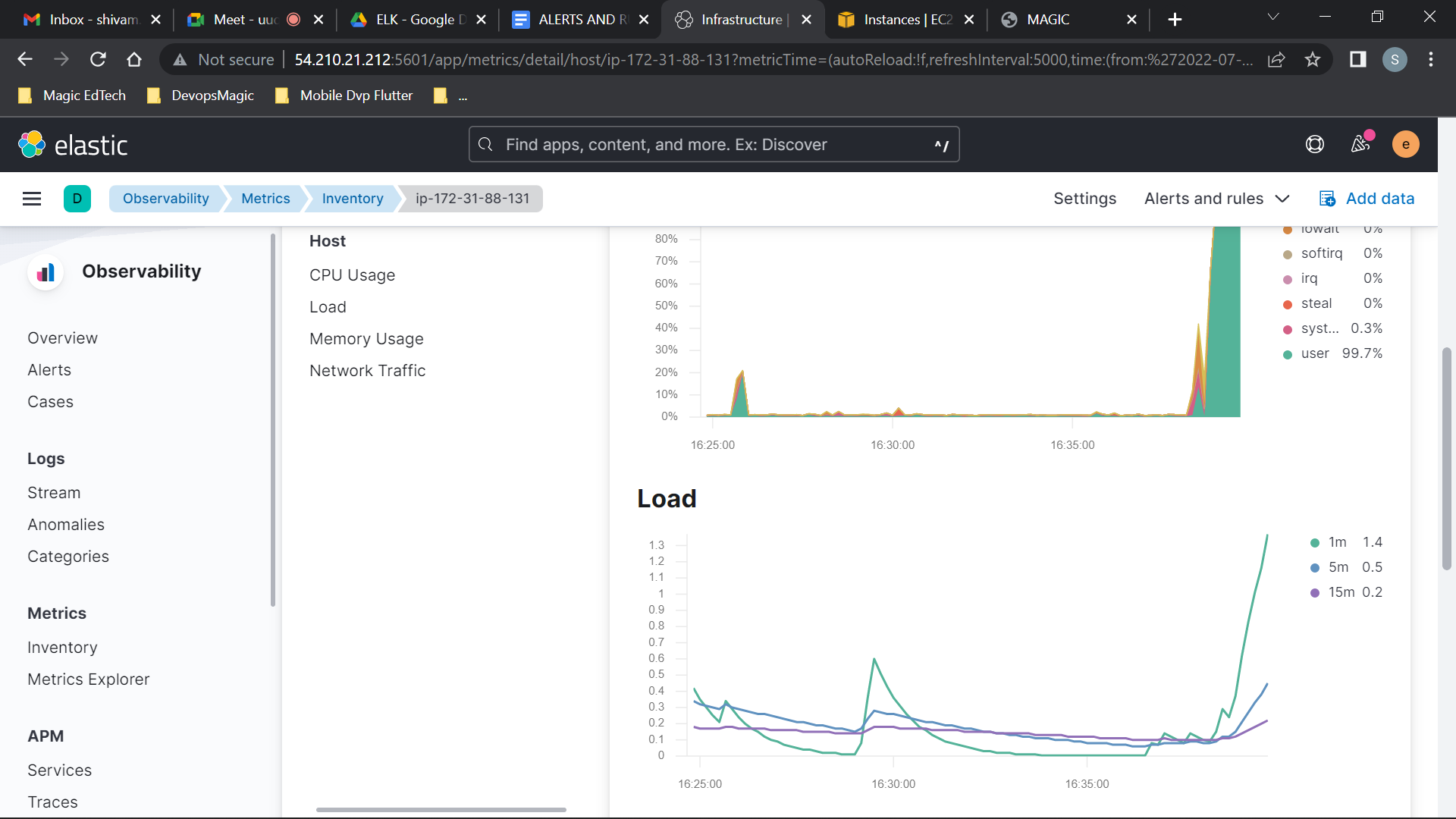
sudo apt install stress

stress --cpu 2 --timeout 60

Alert will become active and after Cpu usage is below threshold alert will be in recovered.

****

****

****